Deutscher Bundestag **Drucksache 19/514**

19. Wahlperiode 18.01.2018

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Konstantin Kuhle, Stephan Thomae, Jimmy Schulz, Manuel Höferlin, Benjamin Strasser, Linda Teuteberg, Grigoris Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Nicola Beer, Dr. Jens Brandenburg, Mario Brandenburg, Dr. Marco Buschmann, Britta Dassler, Bijan Djir-Sarai, Christian Dürr, Dr. Marcus Faber, Daniel Föst, Thomas Hacker, Katrin Helling-Plahr, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Gyde Jensen, Thomas L. Kemmerich, Katharina Kloke, Pascal Kober, Carina Konrad, Wolfgang Kubicki, Michael Georg Link, Oliver Luksic, Dr. Jürgen Martens, Christoph Meyer, Frank Müller-Rosentritt, Dr. Martin Neumann, Dr. Stefan Ruppert, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Katja Suding, Dr. Andrew Ullmann, Gerald Ullrich, Nicole Westig und der Fraktion der FDP

Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung

Nach einer Meldung des Redaktionsnetzwerks Deutschland vom 30. November 2017 plant das Bundesministerium des Innern, die Industrie zu verpflichten, den Sicherheitsbehörden digitale Einfallstore für das Ausspionieren von privaten Autos, Computern, Unterhaltungs- sowie Haushaltsgeräten zu eröffnen (vgl. www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-Autos-Computern-und-Smart-TVs-ermoeglichen, letzter Abruf: 2. Januar 2018).

Dabei gehe es insbesondere um die gesetzliche Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f der Strafprozessordnung (StPO). So solle es etwa für Unternehmen und andere Entwickler künftig eine Auskunfts- und Mitteilungspflicht zur verdeckten Überwindung von Sicherheitssystemen geben. Das Bundesministerium des Innern hat weitreichenden Plänen zur Verpflichtung von Unternehmen und anderen Entwicklern widersprochen. Vielmehr gehe es lediglich um die Hersteller von Alarm- und Sicherheitssystemen (www.zeit.der/digital/datenschutz/2017-12/ueberwachung-wohnraum-de-maiziere).

In den freigegebenen Beschlüssen der 207. Sitzung der Innenministerkonferenz (IMK) am 7. und 8. Dezember 2017 heißt es zum Tagesordnungspunkt 22 (Handlungsbedarf zur gesetzlichen Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f StPO):

> „2. [Die IMK] stellt fest, dass die fortschreitende Entwicklung im Bereich der Fahrzeug- und Schlosstechnik die verfügbaren technischen Möglichkeiten zur verdeckten Überwindung dieser Systeme einschränkt. Dadurch können rechtlich zulässige Maßnahmen nicht umgesetzt werden.

> 3. Die IMK sieht unter Berücksichtigung der im Bericht aufgezeigten Szenarien und aus Gründen der Rechts- und Handlungssicherheit einen weitergehenden Prüfbedarf im Hinblick auf technische und rechtliche Lösungsmöglichkeiten zur Umsetzung der Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f StPO. Insbesondere soll dabei geprüft werden, ob und inwieweit Dritte beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen zur Mitwirkung de lege lata und de lege ferenda verpflichtet werden können, wobei es ausdrücklich nicht um den Einbau von sogenannten Hintertüren in informationstechnische Systeme geht. Die zu erarbeitenden Lösungen sollten technikoffen ausgestaltet sein.“

Die Berichte im Vorfeld sowie der Beschluss der Innenministerkonferenz haben in betroffenen Kreisen zu großer Verunsicherung geführt.

Auch das Thema „Internet der Dinge“ hat bei der 206. und 207. Sitzung der IMK eine Rolle gespielt. Die 206. IMK hatte die länderoffene Arbeitsgruppe Cybersicherheit beauftragt, die Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge umfassend zu prüfen. Zur 207. Sitzung hat diese Arbeitsgruppe einen Sachstandsbericht veröffentlicht (verfügbar unter www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2017-12-07_08/anlage-zu-top-8.pdf?__blob=publicationFile&v=3, letzter Abruf: 2. Januar 2018).

In diesem Sachstandsbericht heißt es u. a., dass die IMK feststelle, „dass die massenhafte Verbreitung von mit dem Internet verbundenen Gebrauchsgeräten (Internet der Dinge) ohne ausreichende Sicherheitsvorkehrungen eine erhebliche Bedrohung für den Cyberraum darstelle“ und dass „eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge“ erforderlich sei.

In der durch das Bundesministerium des Innern veröffentlichten Cyber-Sicherheitsstrategie für Deutschland 2016 heißt es ferner, das „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten“ spiele bei der Schaffung des notwendigen IT-Sicherheitsniveaus eine „wesentliche Rolle“.

Wir fragen die Bundesregierung:

1. Welcher gesetzgeberische Handlungsbedarf besteht aus Sicht der Bundesregierung, um Dritte zur Durchführung von Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f StPO im staatlichen Auftrag oder zur Ermöglichung solcher Maßnahmen zu verpflichten?
2. Sollte nach Auffassung der Bundesregierung eine neue Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f StPO technikoffen ausgestaltet sein?

   Wenn ja, warum?
3. Wie bewertet die Bundesregierung die Sorge, dass durch eine technikoffene Ausgestaltung der Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung ein potentiell weitreichender Zugang auf private Gebrauchsgeräte möglich wird?

Vorabfassung - wird durch die lektorierte Version ersetzt.

4. Sollte eine neue Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung auf die Hersteller von Alarm- und Sicherheitssystemen beschränkt sein?

   Wenn ja, warum?

   Wenn nein, warum nicht?

5. Wie kann eine gesetzliche Regelung zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nach Auffassung der Bundesregierung gleichzeitig technikoffen und auf die Hersteller von Alarm- und Sicherheitssystemen beschränkt sein?

6. Welche Regelungen sollen nach Auffassung der Bundesregierung bei einer neuen Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung den Grundrechtsschutz durch Verfahren sicherstellen?

   Wie sollen bei einer solchen Maßnahme die Risiken berücksichtigt werden, die anderen Bürgerinnen und Bürgern durch das Unterlassen der Schließung von Sicherheitslücken drohen?

7. Wie geht die Bundesregierung mit Informationen um, welche die IT-Sicherheit von Hard- oder Software betreffen? Werden diese Informationen verwendet, um den verdeckten Zugriff auf informationstechnische Systeme oder andere Geräte zu ermöglichen oder zu erleichtern?

   Werden diese Informationen umgehend an BSI weitergeleitet?

   Wenn nein, wer entscheidet dies nach welchen Kriterien?

8. Welche Sanktionen sollen nach Auffassung der Bundesregierung gegen solche Privaten verhängt werden können, die der Verpflichtung zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nicht nachkommen?

9. Wie will die Bundesregierung sicherstellen, dass die technische Schaffung von Möglichkeiten der verdeckten Informationsgewinnung bei Privaten keine Zugriffsmöglichkeiten für Unbefugte eröffnet?

10. Mit welchen Maßnahmen gedenkt die Bundesregierung die Einrichtungen der öffentlichen Verwaltung vor Zugriffen Unbefugter zu schützen, die gerade auf der Grundlage der technischen Schaffung von Möglichkeiten der verdeckten Informationsgewinnung bei Privaten entstehen?

11. Teilt die Bundesregierung die Feststellung der Innenministerkonferenz, dass eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge notwendig ist?

    Welche Maßnahmen sind aus Sicht der Bundesregierung auf nationaler Ebene erforderlich?

    Welche Maßnahmen sind aus Sicht der Bundesregierung auf europäischer Ebene zu ergreifen?

12. Wie wäre aus Sicht der Bundesregierung eine allgemeine Auskunfts- und Mitteilungspflicht zur verdeckten Überwindung von Sicherheitssystemen mit dem Ziel der Verbesserung der Cybersicherheit vernetzter Geräte („Internet der Dinge“) vereinbar?

13. Wie ist aus Sicht der Bundesregierung eine technikoffene Mitwirkungspflicht Privater beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen mit dem Ziel der Verbesserung der Cybersicherheit vernetzter Geräte („Internet der Dinge“) vereinbar?

Vorabfassung - wird durch die lektorierte Version ersetzt.

14. Wie plant die Bundesregierung, das in der Cyber-Sicherheitsstrategie für Deutschland 2016 definierte Ziel, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus“ zu gewährleisten, mit Blick auf das „Internet der Dinge“ zu verwirklichen?
15. Wie wäre aus Sicht der Bundesregierung eine allgemeine Auskunfts- und Mitteilungs- oder Mitwirkungspflicht zur verdeckten Überwindung von Sicherheitssystemen mit dem Ziel vereinbar, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus“ zu gewährleisten?
16. Wie ist aus Sicht der Bundesregierung eine technikoffene Mitwirkungspflicht Privater beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen mit dem Ziel vereinbar, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus zu schaffen?
17. Welche verfassungsrechtlichen Grenzen bestehen aus Sicht der Bundesregierung für eine Verpflichtung Privater (u. a. Hersteller von Alarm- und Sicherheitssystemen sowie generell von anderer Hard- und Software, einschließlich vernetzter Geräte)zur Durchführung oder Ermöglichung verdeckter Maßnahmen der Informationserhebung?

Berlin, den 16. Januar 2018

Christian Lindner und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333